Honorable Thomas S. Zilly

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

OMNI INNOVATIONS, LLC, a Washington Limited Liability company,

Plaintiff,

v.

INSURANCE ONLY, INC.; MICHAEL WEDEKING, and his marital community; PATRICK WEDEKING, and his marital community,

Defendants.

NO. CV06-1210TSZ

DECLARATION OF BRETT SHAVERS IN SUPPORT OF DEFENDANTS' OPPOSITION TO PLAINTIFFS' MOTION FOR PARTIAL SUMMARY JUDGMENT FOR INJUNCTIVE RELIEF

I, Brett Shavers, declare as follows:

1. I am over the age of 18 and competent to testify as a witness in this matter. I make the following declaration based on personal knowledge and expertise in computer forensics developed over many years.

2. I am a specialist in the area of computer forensics, and have assisted in the planning, collection and analysis of electronically stored information in matters ranging from state and federal criminal cases to class action litigation. I have conducted computer forensics services for criminal investigations, employment matters, intellectual property theft, and other civil matters for law firms, corporations, and city and state governments. I have been assigned to criminal investigations since 1992 as a law enforcement officer and subsequently employed in the private sector with NTI (New Technologies Incorporated) in 2006. I have provided opinions in at least one federal class action litigation involving electronic data in the United States District Court, Northern District of Texas. I have provided opinion testimony in other cases on over 20 occasions. This testimony has occurred in municipal, county, and federal courts in Washington State. No attorney has ever challenged my testimony on the grounds that I was not a competent specialist in any field.

3. My educational and professional background is as follows: I am a graduate of Bellevue Community College with an AAS degree. I have been employed as a commissioned law enforcement officer in Washington State for 14 years, during which I received over 2000 hours of professional training. Over 1000 hours of this training has been in the field of computer forensics investigations, to include e-mail, internet, and network investigations. Subsequent to my law enforcement career, I was employed as a Managing Principal for NTI, leading up to my current position as President of a computer forensic company. In both private positions, I have continued my law enforcement computer forensic investigations into the private sector.

4. I have been retained by the law firm of Rettig, Osborne, Forgette, O'Donnell, Iller & Adamson, LLP, to provide my expert opinions regarding certain factual matters in this case, especially regarding the typical steps required to be followed to authenticate and prove the transmission and receipt of e-mails, especially in the context of "spam" e-mails.

5. To describe the process to authenticate and prove the transmission and receipt of e-mails, a brief explanation of relevant information is needed. E-mails consist of three components: header, body and attachment. Of these three components, the header should contain the information needed to begin investigating an e-mail. The header consists of several components, some of which are: sender e-mail address, receiver e-mail address, subject, time of creation, delivery stamps, message author, cc (carbon copy), bcc (blind carbon copy). It is through the analysis of the header that an investigation can be conducted to find the origination and destination of an e-mail. One of the most pertinent parts of the header is the "route" of the e-mail that has been documented. The route of an e-mail as it travels from origin to destination is not unlike the route of typical postal mail, as it is usually not delivered directly without several stops along the way. These electronic stops consist of passing through the sender's mail server (whether it be internet based, such as webmail, or intranet based, such as through a company e-mail system), out to the internet, through one or more "re-mailers," to the receiver's e-mail server, and finally to the receiver's computer. Through this route, the e-mail will more than likely travel through firewalls as well.

6. The e-mail route is being documented as it travels through the internet to its final destination. The information contained may have been

forged by the sender in various manners. The forgery of an e-mail header can include false internet protocol (IP) addresses (the origin address is faked as an example), false return e-mail address, false author, and other items a sender can employ to reduce the risk of being disclosed as the sender. Senders may also employ the use of 'zombie' computers to relay e-mail. A zombie computer is an innocent computer user on the internet that has been intentionally infected with a virus unbeknownst to that computer user. This zombie computer is able to receive e-mails and relay them to their destination without the zombie computer user being aware. Hundreds of thousands of e-mails can be forwarded by a single zombie computer in short periods of time. Tracking the origin of an e-mail that has been relayed by one or more zombie computers is extremely difficult, if not impossible. Additionally, legitimate e-mail relay hosts may not place enough information in the e-mail header to identify the sender or route.

7. Prior to the receiver being able to read the e-mail on its arrival, there may be automated processes in play with the receiver's computer. Most e-mail account service providers and e-mail software applications provide settings for filters and scanning that are intended to find, sort, and/or filter various incoming e-mails for viruses, Trojans, and spam e-mail. Upon receipt of any of these types of e-mails, the receiving software application or e-mail server may be directed to alter the e-mail in some way per user choice or software default settings. These settings may include deletion, quarantine, or alteration of the e-mails in order to protect the receiving computer system from harm.

8. In the acquisition of electronic evidence, certain procedures are observed to obtain "best evidence." These procedures are based upon the type of electronic evidence being acquired and the media from which it is being

acquired. No matter which type or where stored, a basic premise is to "do no harm" during the acquisition, so that the data that is acquired is an identical copy of the original. In the case of e-mail acquisitions, there are several factors that exist that must be accounted for to obtain best evidence, as it is not typical that the original e-mail from the sender is acquired.

9. To obtain the best evidence, capturing the e-mail server logs from both the sender and receiver would be the most accurate method. This method would provide a basis to show the original untouched e-mail that was sent, and compare it to the received e-mail. This is not always possible; therefore, capturing the e-mail and e-mail logs (a log being a documented e-mail history) from the receiver's server or the sender's server would be second best. Notwithstanding that many users have web-based e-mail accounts, access to these servers may not be easy or possible. Therefore, acquiring the e-mail would entail risking some alterations depending upon the receiver's e-mail default or user settings. This could include altering the subject lines, stripping information from the body or attachments, as well as not showing complete header information. Simply copying or saving an e-mail onto a media storage device such as a floppy, CD rom, or hard drive may not completely or accurately capture the e-mails. Additionally, saved e-mails may intentionally be altered by a user after being saved to external media, sometimes due to improper motivations of the user. Without access to the receiving computer or original email logs, this alteration would be nearly impossible to detect if only given the copied emails on external media.

10. The best practice would then require access to server logs if they exist as well as access to the e-mail account settings to determine what, if any,

alterations were configured. Copies of the e-mails would need to have the complete header information included as well. Authentication of the e-mail's travel route would require verifying each of the "stops" (re-mailers) addresses to determine if any forged addresses were used as well as if any zombie computers were part of the e-mail route. To give credibility to any acquisition of digital media, neutral third party vendors or appointed Special Masters should be used in the verification and authentication of acquired data.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

SIGNED at Bellevue, Washington, on this 3rd day of July, 2007.

BRETT SHAVERS

CERTIFICATE OF SERVICE

I hereby certify that on July 9, 2007, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system which will send notification of such filing to the following: Robert J. Siegel, and I hereby certify that I have mailed by United States Postal Service the document to the following non CM/ECF participants: N/A.

s/ Cheryl R.G. Adamson / WSBA #19799
Attorney for Defendants
RETTIG OSBORNE FORGETTE, LLP
6725 W. Clearwater Avenue
Kennewick, WA 99336
Phone: (509) 783-6154
Fax: (509) 783-0858
E-mail: cheryl.adamson@rettiglaw.com